



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/788,295	02/16/2001	Stephan W. Gehring	FANT-P019	1506
44279	7590	04/06/2006	EXAMINER	
PULSE-LINK, INC. 1969 KELLOGG AVENUE CARLSBAD, CA 92008			SON, LINH L D	
			ART UNIT	PAPER NUMBER

2135

DATE MAILED: 04/06/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

DETAILED ACTION

1. This Office Action is responding to the Amendment received on 01/05/06.
2. Claims 1, 5 are amended. Claims 2 and 6 are canceled.
3. Claims 1, 3-5, 7-17, and 19-23 are pending.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. **Claims 1-10, 14, and 19-23 are rejected under 35 U.S.C. 102(e) as being anticipated by Jakobsson, US Patent No. 6587946.**
6. As per **claims 1**, Jakobsson discloses "A method for forwarding messages in a multi-node network (Col 6 line 58 to Col 7 line 20 (multi-proxy servers and e-mail clients)) comprising decrypting, by any forwarding node (Proxy servers), any message

Art Unit: 2135

received by said any forwarding node and encrypting each message transmitted by said any forwarding node." in (Col 6 line 58 to Col 7 line 20, Col 6 lines 3-25, and Col 6 lines 40-48)

7. As per **claims 3-4, 7-8, and 22-23**, Jakobsson discloses "the method of claims 2, 6, and 21, wherein said encrypting said message by said source node, said decrypting of said transmitted message by said any forwarding node, said re-encrypting of said decrypted message by said any forwarding node, and said decrypting of said re-encrypted message by said destination node, are carried out using asymmetrical/symmetrical encryption and decryption" in (Col 6 lines 30-48, and Col 1 lines 30-43, and Col 2 line 60 to Col 3 line 8).

8. As per **claim 5**, Jakobsson discloses "A method for forwarding messages in a multi-node network (Col 6 line 58 to Col 7 line 20 (multi-proxy servers and e-mail clients)) comprising decrypting, by any forwarding node, any message received by said any forwarding node prior to determining a destination for said received message and encrypting each message transmitted by said any forwarding node." in (Col 6 line 58 to Col 7 line 20, Col 6 lines 3-25, and Col 6 lines 40-48).

9. As per **claim 6**, Jakobsson discloses "The method of claim 5, further comprising encrypting, by said any forwarding node, each message transmitted by said any

Art Unit: 2135

forwarding node" in (Col 6 line 58 to Col 7 line 20, Col 6 lines 3-25, and Col 6 lines 40-48).

10. As per **claims 9, and 14**, Jakobsson discloses the "Cryptographic Communication System" invention, which includes a method for encrypting and decrypting messages in a multi-node network" in (Col 6 line 58 to Col 7 line 20), comprising: (a) encrypting a message by a source node and transmitting said encrypted message to any forwarding node (Col 5 lines 18-25); (b) receive the message, decrypting said encrypted message by said any forwarding node (Col 6 lines 3-30, Col 5 lines 18-65); (c) re-encrypting said decrypted message by said any forwarding node and transmitting said re-encrypted message to a destination node (Col 8 lines 9-23, and Col 8 lines 25-68); and (d) receiving and decrypting said re-encrypted message by said destination node" in (Col 8 lines 55-60, and Col 8 lines 25-65).

11. As per **claims 10**, Jakobsson discloses "The method of claim 9, wherein said encrypting said message by said source node, said decrypting of said transmitted message by said any forwarding node, said re-encrypted message by said destination node, are carried out using symmetrical encryption and decryption" in (Col 6 lines 30-48, and Col 1 lines 30-43, and Col 2 line 60 to Col 3 line 8).

Art Unit: 2135

12. As per **claim 19**, Jakobsson discloses "An encryption and decryption system for a multiple node network (Col 6 line 58 to Col 7 line 20 (multi-proxy servers and e-mail clients)), comprising a plurality of nodes (multi-proxy servers), with each of the plurality of nodes including means for decrypting all received messages, and means for encrypting all transmitted messages" in (Col 6 line 58 to Col 7 line 20, Col 6 lines 3-25, and Col 6 lines 40-48).

13. As per **claims 20**, Jakobsson discloses the encryption and decryption system of claim 19, further comprising at least one source node, said source node including means for encrypting messages and transmitting said encrypted messages to said any forwarding node (Col 6 line 58 to Col 7 line 20).

14. As per **claims 21**, Jakobsson discloses the encryption and decryption system of claim 20, further comprising at least one destination node, said destination node including means for decrypting messages transmitted by said any forwarding node (Col 8 lines 55-60, and Col 8 lines 25-65).

Claim Rejections - 35 USC § 103

15. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

16. **Claims 11-13, and 15-17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jakobsson and further in view of Mitty et al, US Patent No. 6199052, hereinafter "Mitty".**

17. As per **claims 11 and 15**, Jakobsson discloses the method of claims 10 and 14. Further Jakobsson discloses "(c) said decrypting of said transmitted message by said any forwarding node is carried out using a second key; and (d) said re-encrypting of said decrypted message by said any forwarding node is carried out using said second key" in (Col 6 lines 3-30, Col 5 lines 18-65, Col 8 lines 9-23, and Col 8 lines 25-68).

However, Jakobsson is silent on "wherein: (a) said encrypting said message by said source node is carried out using a first key; (b) said decrypting said re-encrypted message by said destination node is carried out using said first key";

Nevertheless, Mitty discloses the "Secure Electronic Transactions Using A Trusted Intermediary with Archive and Verification Request Services" invention, which teaches a method of sending the a message securely between the sender and the receiver

Art Unit: 2135

through an intermediary. The message M1 gets encrypted first with the sender private key to form M2. Then get encrypted a couple more times with certification and key information and further encrypted again at the 5th time using the public key of the intermediary before send the M6 encrypted message to the intermediary (forwarding node) (Col 9 line 12 to Col 10 line 65). The M6 message gets decrypted with the intermediary's private key to process the message M5 according and identify the destination. The intermediary does not have the public key of the sender to decrypt all the level of encryption. The message M5 then becomes M7 after processing (Col 11 lines 44-55). Then M7 gets encrypted with more information a couple more rounds until the last round, M10, where the M9 message gets encrypted with the recipient's public key (Col 11 lines 43 to Col 12 line 65). The message M9 then gets decrypted multiple times for verification of originality until it gets to the text message M2, which the receiver would use the sender's public key to decrypt to clear text (Col 13 lines 1-10). As Mitty discloses, the key to encrypt the original text message and the key to decrypt the encrypted message is only the first key.

Therefore, it would have been obvious at the time of the invention was made for one having ordinary skill in the art to incorporate the invention of Mitty with Jakobsson with the motivation of protecting the privacy of the message from the intermediary or forwarding node by not sharing the knowledge of the encrypting key of the message.

18. As per **claims 12 and 16**, Jakobsson and Mitty disclose "the method of claims 11 and 15, wherein said second encryption/decryption key is different from said first

Art Unit: 2135

encryption/decryption key" in (Mitty, Col 8 lines 20-34, Col 10 lines 10-27, and Col 13 lines 1-10).

19. As per **claims 13 and 17**, Jakobsson and Mitty discloses "the method of claim 11, wherein said second encryption/decryption key and said first encryption/decryption key are the same" in (Mitty, Col 3 lines 43-50).

Response to Arguments

20. Applicant's arguments filed 01/05/06 have been fully considered but they are not persuasive.

21. As per remark on page 8, Applicant argues that "Thus this aspect of Jakobsson teaches decrypting a message without subsequently encrypting, or re-encrypting the message" in relying on

"Theoretical asymmetric proxy encryption, where the proxy is one physical party, and the proxy has the key that allows him to decrypt the transcript. Such a solution requires a certain amount of trust, since the proxy is able to read the messages sent to the primary recipient. Therefore, this type of solution appears to be advantageous mainly as a means for speed-up due to merging the decrypting and encrypting operations into one operation" (Col 6 lines 31-39).

Art Unit: 2135

Examiner respectfully disagrees with the Applicant. According to Jakobsson's invention, the secret decryption key is allocated into three shares for use by three proxy servers. However, upon decrypting the message using said share decryption key, participating proxy servers can read the message and re-encrypting the message back to its original encrypted message by combining the separate transforms of the message from each server. (See Col 7 lines 30-45, and Col 8 lines 9-13). By the broadest interpretation of the claim language, Jakobsson's teaching does decrypting the message by any forwarding node, and re-encrypting decrypted message, by any one set of proxies, by the act of combining the separate transforms of the message from each proxy server (See Col 7 lines 30-45, and Col 8 lines 9-13). A set of proxies in Jakobsson's invention is corresponding to the node claimed.

22. As per remark on page 8 (Jakobsson also teaches decryption that is only decryptable by the secondary recipient: ... The proxy server does not decrypt the message, but instead, adds an additional encryption key, and passes the message on to a secondary recipient, who then decrypts the message.), Applicant argues the proxy server does not decrypt the message. Again Applicant relies on the conclusion in Col 3 line 59 to Col 4 line 3. Examiner believes that the Applicant misinterprets the cited Cols and lines above. In Col 3 line 59 to Col 4 line 3, Jakobsson teaches of modifies the message by using the individual share of the key portion to decrypt the encrypted message. Since each proxy server can only see a portion of the message, the

Art Unit: 2135

message is hidden as a whole to the proxy server. Such interpretation is elaborated and clearly explained in Col 7 lines 20-45.

23. Therefore, the rejection basis dated 01/06/05 is maintained.

Conclusion

24. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

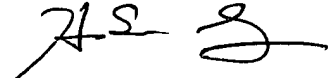
Art Unit: 2135

25. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Linh LD Son whose telephone number is 571-272-3856. The examiner can normally be reached on 9-6 (M-F).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Linh LD Son
Examiner
Art Unit 2135


HOSUK SONG
PRIMARY EXAMINER